Sudden Increase in ICMP Traffic

IEPG Meeting, Prague, CZ, 18 March 2007

Simon Leinen, SWITCH
<simon@switch.ch>

Background

Academic network provider (AS559)

- About 2.5 Gb/s external traffic
- Announcing 91 prefixes, including 30 /16 + 3 /15

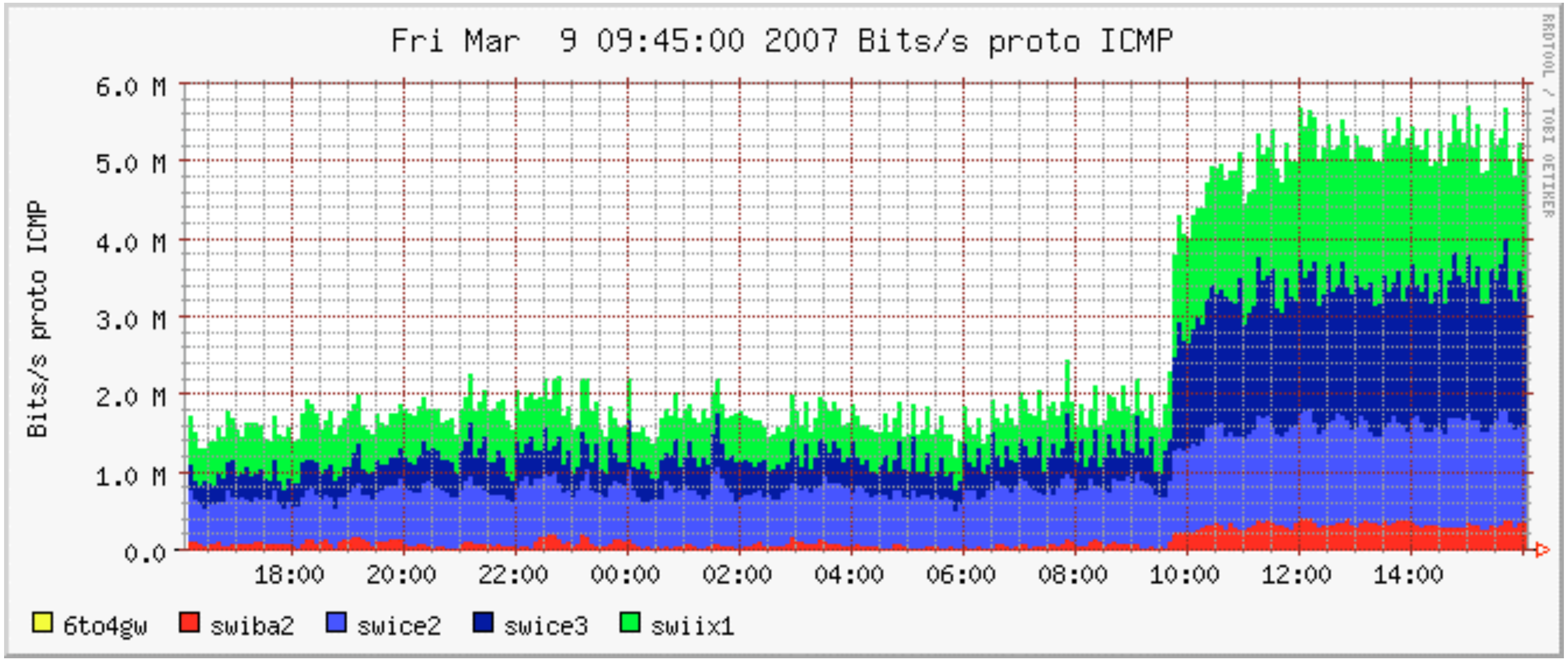
Unsampled NetFlow exported from four external border routers

Raw flows archived for network operations and security analysis

- NFDUMP/NfSen toolset (http://nfsen.sf.net/)

Friday morning a week ago...

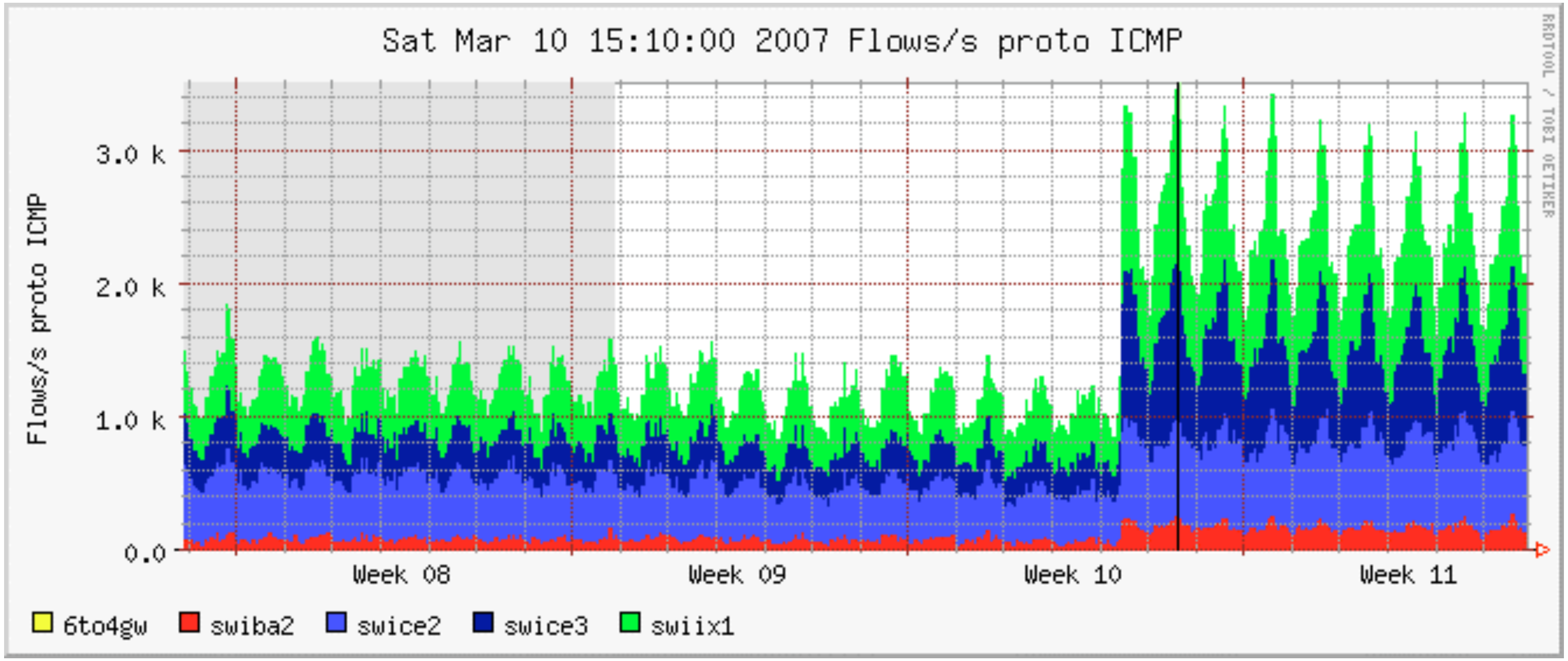
Starting at 08:42:45 UTC on 9 March 2007, we saw an increase in incoming ICMP traffic to our network (AS559)



This graph shows bps of ICMP traffic, from unsampled NetFlow export from our external border routers (pps and fps look very similar)

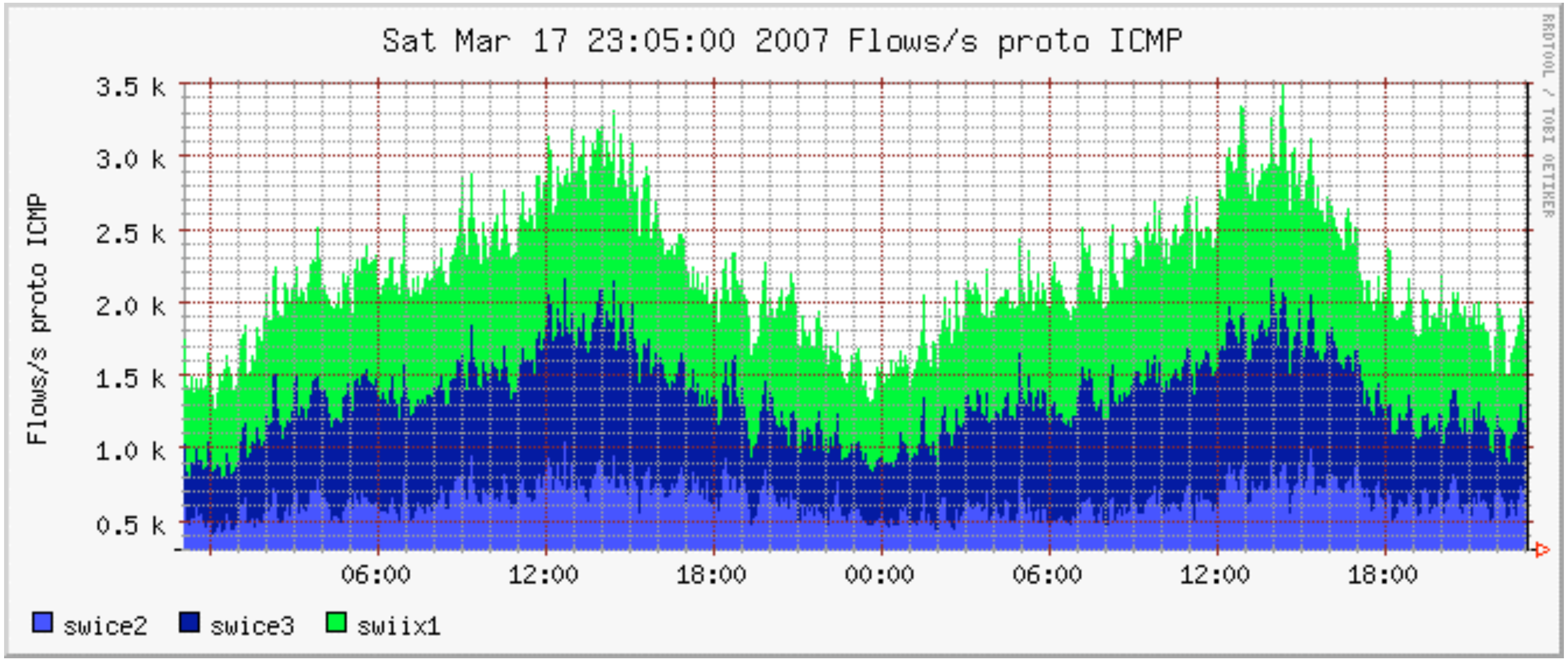
More than week later...

...ICMP traffic remains at this unusually high level



First observations about new ICMP traffic

- Traffic seems to go to all customers
  - That turned out to be wrong: only 13 /16s (out of our 36+) are targeted
  - Open question: How were these chosen?
- Traffic seems to come from all commercial upstreams
  - Most of it from China; see the dominating day-curve



First observations on new ICMP traffic (2)

- Traffic usually consists of 4*60 bytes of ICMP Echo requests
  - Similar to Windows “ping” fingerprint
  - But Echo requests stop when there is an ICMP Echo response
- Seems to be part of scanning
  - When a host responds, it is sent a TCP packet to port 445
  - Why not scan for TCP port 445 right away? (Not stealth enough?)
- Possibly a worm
  - an “Allaple” variant was suggested, see http://isc.sans.org/diary.html?storyid=2451

Open Questions (1)

- Is this an Internet-wide event?
  - I think so, friends in other countries have been seeing this as well
  - But then others have not, even one with /8 background-radiation telescope
  - Where's the Abilene Weekly NetFlow report when you need it?

Open Questions (2)

- What caused the fast ramp-up?
  - Were many systems infected at once,
  - or was an existing compromised population triggered/upgraded?

Open Questions (3)

- What is the propagation strategy (presuming this is a worm)?
  - How are the targets chosen?
  - Why probe with ICMP first?

Open Questions (4)

SWITCH
The Swiss Education & Research Network

- Should we be worried about this?
  - Probably not – ICMP is still a tiny fraction of traffic
  - And these episodes may be quite common
  - Might cause some ICMP rate-limits to be tripped (but those will be tripped anyway as traffic grows, because nobody ever updates them)-:
  - Might cause problems near the sending end where infections are high
  - If this is really “Allaple”, that worm does perform a DdoS against someone.

Open Questions (5)

- Assuming that we can detect this within minutes (which sounds quite feasible in this particular case), is there a sensible reaction?
  - Detection of Internet-wide anomalies is often touted as important/useful...

SWITCH

The Swiss Education & Research Network